N° d'enregistrement
au C.N.R.S.
AO 1878.

ARTICLE PRINCIPAL

Recouvrant en tout

LA THESE DE DOCTORAT ES-SCIENCES-MATHEMATIQUES

présentée

A LA FACULTE DES SCIENCES

de PARIS

PAR

M. RICHALET Jacques

pour obtenir

le grade de Docteur Ès-Sciences

Sujet de la Thèse : "Calcul opérationnel dans un anneau fini et systématique discrète"

soutenue le 20 Décembre 1967 devant la commission d'Examen

MM. J.VILLE Président
P.OLMER Examinateurs
M.PELEGRIN

OPERATIONAL CALCULUS FOR FINITE RINGS

J. RICHALET

Reprinted from IEEE TRANSACTIONS ON *CIRCUIT THEORY*
Vol. CT-12, Number 4, December 1965
Pp. 558-570
Copyright 1965, and reprinted by permission of the copyright owner
PRINTED IN THE U.S.A.

UNIV.
LEIDEN
BIBL.

Operational Calculus for Finite Rings

J. RICHALET, MEMBER, IEEE

***Abstract*—By means of the theory of Galois fields and formal series, it is possible to develop an operational calculus for the finite sequence space of finite fields and rings, where group laws are modulo k sum and product; whether k is prime or not. The sequences that can be treated are ultimately periodic. Elementary properties of this calculus are given and application to linear sequential systems is made possible by the introduction of transfer functions. Examples are described where the proposed calculus can be used to advantage.**

Manuscript received May 6, 1964; revised August 10, 1965.
The author is with the Centre d'Études et de Recherches en Automatisme, École Nationale Supérieure de l'Aéronautique, Paris, France.

INTRODUCTION

AT FIRST GLANCE there may seem to be a gap between classical control theory and switching theory. However, if the theories appear to be different, this difference lies in approach rather than in content. It is possible to go from continuous control systems to sequential logic via sampled data and quantized systems. If the number of values that can be taken on by a variable of a finite-state machine is two, we are in the domain of Aristotelian logic. If it is more than two, we are dealing with a non-Aristotelian logic such as that

introduced by the Polish school of Lukasiewicz in 1920. It then appears that we can consider a finite-valued system either as a usual sampled and quantized system or as an n-valued sequential logic system. Thus the sequential logic and control theories are akin, both being aspects of the general theory of the systems. The advantages of a unified approach are pointed out in [11].

Combinational and sequential logics, equipped with the group postulates (such as the modulo two sum or logical product), are consistent with the laws of algebra as well as the premises of control system theory. A basic question which arises in this connection is whether it is possible to develop an operational calculus applicable to a finite Abelian field or ring which will be analogous to Laplace's operational calculus.

Polynomial representations and even transfer functions for binary systems have been developed by many authors [6]–[10]. Their aim was mainly to obtain a representation of binary sequences, not an operational calculus. Coding theory has used extensively state representation theory and matrix calculus. However, the relationship between state space techniques and transfer function techniques has not been fully explored to the author's knowledge.

I. Operational Calculus

A. Galois' Theorem in a Finite Field

Let us consider polynomials $G(p)$ of degree n where p is an indeterminate and the coefficients are elements of Z_k.[1] Galois asserts that there exist a polynomial $C(p)$ and a number q such that for every $G(p)$ with a constant term

$$G(p)\cdot C(p) = p^q - 1 \quad \text{with} \quad q \leq k^n - 1 \qquad (1)$$

as the coefficients of $G(p)$ are elements of Z_k; (1) becomes

$$G(p)\cdot C(p) = p^q - 1$$
$$= p^q + (k-1) \quad \text{with} \quad q \leq (k^n - 1)$$

The least number q is called the *period* of $G(p)$; if $q = k^n - 1$, $G(p)$ is said to be *primitive*. The polynomial $C(p)$ is called the *complementary* polynomial of $G(p)$. It is often useful to know the period of $G(p)$. Instead of going through the tedious process of dividing polynomials $(p^i - 1)$ by $G(p)$, it is easier to express successive powers of a root a of $G(p)$ in terms of the $(n-1)$ first powers until the identity $a^q = 1$ is attained.

Example (Z_2): $G(p) = p^3 + p + 1$. If a is a root of $G(p)$, powers of a are

$$a^0 = 1, a, a^2, a^3 = a + 1, a^4 = a^2 + a,$$
$$a^5 = a^2 + a + 1, a^6 = 1 + a^2, a^7 = 1.$$

[1] Z_k is the field of integers, modulo k, where k is a prime.

Hence

$$p^7 + 1 = (p^3 + p + 1)\cdot(p^4 + p^2 + p + 1),$$
$$G(p) = (p + a)\cdot(p + a^2)\cdot(p + a^4)$$
$$C(p) = p^4 + p^2 + p + 1 = (p + a^3)\cdot(p + a^5)$$
$$\cdot(p + a^6)\cdot(p + a^7) = (p + 1)\cdot(p^3 + p^2 + 1).$$

If b is a root of $p^3 + p^2 + 1$, $p^3 + p^2 + 1$ is also primitive: $b^3 = b^2 + 1$, $b^4 = b^2 + b + 1$, $b^5 = b + 1$, $b^6 = b^2 + b$, $b^7 = 1$.

B. Operational Calculus in a Finite Field

Let $K[x]$ be the ring of polynomials $P(x)$:

$$P(x) = a_0 + a_1 + \cdots + a_n x^n \qquad a_i \in Z_k$$

where x is an indeterminate. $K[x]$ is contained in the ring $K[[x]]$ of formal series such as $S(x)$

$$S(x) = a_0 + a_1 x + \cdots + a_n x^n + \cdots$$

where multiplication is the ordinary formal multiplication of power series. Let $K(x)$ be the field of rational functions $u(x)/w(x)$ where $u(x)$ and $w(x)$ are elements of $K[x]$.

Proposition 1: *Every polynomial $P'(x)$ with a constant term different from zero, has an inverse in $K[[x]]$.*

Proof:

$$P'(x) = a_n x^n + a_{n-1}x^{n-1}$$
$$+ \cdots a_1 x + a_0 = P(x) + a_0 \qquad (a_0 \neq 0)$$

There exists for every $a_0 \in Z_K$ $a, b \in Z_K$ such that

$$a_0 b = (k - 1).$$

The inverse of $P'(x)$ is

$$a_0^{-1}\cdot \sum_0^\infty [bP(x)]^n = [P'(x)]^{-1}$$

which can be verified as follows:

$$[a_0 + P(x)]\left[a_0^{-1} \sum_0^\infty [bP(x)]^n\right]$$
$$= a_0^{-1}[a_0 + P(x)][1 + bP(x) + b^2P^2(x) + \cdots]$$
$$= a_0^{-1}[a_0 + a_0 bP(x) + a_0 b^2P^2(x) + \cdots$$
$$+ P(x) + bP^2(x) + \cdots]$$
$$= a_0^{-1}\cdot a_0 = 1$$

Let us now consider the field $A(x)$ of rational functions whose denominators $w'(x)$ are polynomials with nonzero constant terms:

$$w'(x) = a_0 + w(x)$$
$$[w(x) = 0]_{x \doteq 0} \qquad a_0 \neq 0.$$

$A(x)$ is a subfield of $K(x)$. If $f(x)$ is a rational function, there exist $u(x)$ and $w'(x)$ (in fact many) such that

$$f(x) = u(x)/w'(x).$$

By proposition 1, it is possible to associate with $f(x) \in A(x)$ some $\phi[f(x)] \in K[[x]]$ in the following way:

$$f(x) = \frac{u(x)}{w'(x)} \rightarrow \phi[f(x)] = u(x)a_0^{-1} \sum_{n=0}^{\infty} [bw(x)]^n$$

where

$$a_0 b = (k - 1).$$

Proposition 2: Φ *is uniquely defined and is an isomorphism from* $A(x)$ *into* $K[[x]]$.

Proof: Clearly Φ is uniquely defined and is also a one-to-one mapping. If $uv^{-1} = u'v'^{-1}$ for the rational functions $f = u/v$ and $f' = u'/v'$, then multiplying by vv we get $uv' = u'v$. Hence

$$f(x) = \frac{u(x)}{v(x)} = \frac{u'(x)}{v'(x)} = f'(x).$$

$\sum(x)$ is the sum of two rational functions $f(x)$ and $f'(x)$:

$$\sum(x) = \frac{u}{v} + \frac{u'}{v'} = \frac{uv' + vu'}{vv'}.$$

$$\Phi[\sum(x)] = (uv' + vu')(vv')^{-1}.$$

With $\sum(x)$ we associate

$$(uv' + vu')(vv')^{-1} = uv^{-1} + u'v'^{-1} = \Phi[f(x)] + \Phi[f'(x)]$$

hence

$$\Phi[\sum(x)] = \Phi[f(x)] + \Phi[f'(x)]$$

and the image of the sum is the sum of the images.

$\prod(x)$ is the product of $f(x)$ and $f'(x)$.

$$\pi(x) = \frac{u}{v} \cdot \frac{u'}{v'}.$$

With $\prod(x)$ we associate

$$\Phi[\pi(x)] = (uu')(vv')^{-1}$$

$$(uu')(vv')^{-1} = (uv^{-1})(u'v'^{-1}) = \Phi[f(x)] \cdot \Phi[f'(x)]$$

hence

$$\Phi[\pi(x)] = \Phi[f(x)] \cdot \Phi[f'(x)]$$

and the image of the product is the product of the images.

Proposition 3: *The image in* $K[[x]]$ *of a rational function is an ultimately periodic series and conversely.*

Proof: Let $f(x) = u(x)/v(x) \in A(x)$. According to Galois' theroem there exists a $w(x)$ and a q such that

$$f(x) = \frac{u(x)}{v(x)} = \frac{u(x)w(x)}{v(x)w(x)} = \frac{u(x)w(x)}{x^q - 1}.$$

The numerator is a polynomial, and thus a periodic series beyond a certain point; $(x^q - 1)^{-1}$ is a periodic series of period q by proposition 1 since

$$(x^q - 1)^{-1} = [x^q + (k - 1)]^{-1}$$

$$= (k - 1)(1 + x^q + x^{2q} + \cdots).$$

The product $u(x) \cdot w(x)(x^q - 1)^{-1}$ is then a periodic series beyond a certain point.

Conversely, a series of ultimate period q, periodic beyond the kth term, can be represented by ($k = q$ for example):

$$S(x) = a_0 + a_1 x + \cdots + a_{K-1}x^{K-1} + [a_K x^K + \cdots a_{2K-1}x^{2K-1}] + a_K x^{2K} + \cdots$$

$$S(x) = a_0 + a_{K+1}x + \cdots + a_{2K-1}x^{K-1} + [a_K x^K + \cdots a_{2K-1}x^{2K-1}] + \cdots + b_0 + b_1 x + \cdots b_{K-1}x^K.$$

$S(x)$ is the sum of a periodic series

$$S'(x) = \sum_{i=0}^{K-1} a_{K+i} \sum_{j=0}^{\infty} x^{Kj+i}$$

and of a polynomial

$$P(x) = \sum_{i=0}^{K-1} b_i x^i$$

where

$$a_i = b_i + a_{K+i}.$$

C. Discrete Laplace transform in the finite sequence space of a finite field

We can readily associate a series with a sequence. At this point we also know how to associate a rational function with an ultimately periodic series.

In accordance with the isomorphism indicated by proposition 2, we shall identify ultimately periodic series with rational functions and write [2]

$$A(x) = \frac{a_0 + a_1 x + \cdots a_K x^K}{1 + x^q} = a_0 + a_1 x + \cdots a_n x^n + \cdots. \quad (2)$$

In order to be consistent with the existing operational calculus, we shall change variables ($p = 1/x$) and multiply equation (2) by x. We obtain:[2]

$$A^*(p) = \frac{a_0}{p} + \frac{a_1}{p^2} + \cdots \frac{a_i}{p^{i+1}} = \sum_{i=0}^{\infty} \frac{a_i}{p^{i+1}}.$$

Let v be an infinite sequence $[v(n)]$ of elements of Z_k. We associate with this sequence v the formal series $V(p)$

$$V(p) = \frac{v(0)}{p} + \frac{v(1)}{p^2} + \cdots \frac{v(n)}{p^n} + \cdots = \sum_{0}^{\infty} \frac{v(n)}{p^{n+1}}. \quad (3)$$

[2] This change of variable will be justified in Section I-G. Division by p cancels the factor p appearing the numerator of most commonly used transforms.

Definition: $V(p)$ *is the discrete Laplace transform modulo* k *of the sequence* v.

This provides us with the contemplated operational calculus. When v is an ultimately periodic series we know [see (2)] how to "sum" the series, or write it in a closed form. $v(n)$ and $w(n)$ denote series with period q where periodicity starts immediately and after h terms, respectively:

$$v(n) = [v(0)v(1) \cdots v(q-1)]$$

$$w(n) = b(0)b(1) \cdots b(h-1)[w(0)w(1) \cdots w(q-1)].$$

$w(n)$ is said to be "q-periodic from term h". We shall denote the discrete Laplace transform of $v(n)$ as $V(p)$; $v(n) \subset V(p)$. The canonical form of $V(p)$ is:

$$V(p) = \frac{v(0)p^{q-1} + v(1)p^{q-2} + \cdots v(q-1)}{p^q - 1} \tag{4}$$

$$W(p) = \frac{a(0)p^{q+h-1} + a(1)p^{q+h-2} + \cdots + a(q+h-1)}{p^h(p^q - 1)}. \tag{5}$$

Examples: a) (Z_2)

$$v_1(n) = [1] \subset \frac{1}{p+1} \qquad v_2(n) = [0\ 1] \subset \frac{1}{p^2+1}$$

$$v_3(n) = 1\ 1[0\ 1] \subset \frac{p^2+p+1}{p(p^2+1)}$$

The following example clearly demonstrates the advantages of Galois' theorem:

$$v_4(n) = [0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0$$
$$\cdot 1\,0\,0\,1\,1\,1\,1\,0\,1\,0\,0\,0\,1\,1\,1\,0\,0\,1\,0\,0\,1\,0\,1$$
$$\cdot 1\,0\,1\,1\,1\,0\,1\,1\,0\,0\,1\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,1\,1]$$

$$V_4(p) = \frac{1}{p^6+p+1}$$

b) (Z_3)

$$v_5(n) = [1] \subset \frac{1}{p+2} \qquad v_6(n) = [0\ 2] = \frac{2}{p^2+2}$$

$$v_7(n) = [0\ 1\ 2] \subset \frac{p+2}{p^3+2} = \frac{1}{p^2+p+1}.$$

D. Extension of Galois' theorem

If k is not a prime number, Z_k is a ring with some elements being zero divisors. Galois' theorem is no longer true in its original form and the theory must be modified.

Let us consider polynomials of the form

$$G(p) = a_n p^n + a_{n-1}p^{n-1} + \cdots a_0$$

where a_n has an inverse in Z_k

$$a_n \cdot b = 1 \qquad (a_n \neq 0,\ b \neq 0,\ a_n \cdot b \neq 0)$$

and let us perform the formal division $1/G(p)$

$$a_n p^n + a_{n-1}p^{n-1} + \cdots + a_0 \qquad \frac{a_n^{-1}}{p^n} + \cdots + \qquad = Q(p)$$

$$1 \qquad\qquad\qquad\

Conversely, it is possible to associate with a rational function: $N(p)/D(p)$ $[D(p) = a_n p^n + \cdots + a_0]$ where:

$$\text{degree of } N(p) < \text{degree of } D(p)$$

and where a_n has an inverse ($a_n \cdot b \neq 0$, $b \neq 0$), an ultimately periodic series:

$$\frac{N(p)}{D(p)} = \frac{N(p)C(p)}{p^q(p^{q'} - 1)}.$$

Examples (Z_4):

$$v_1(n) = [1] \subset \frac{1}{p+3}$$

$$v_2(n) = [0\ 1\ 2\ 3] \subset \frac{p^2 + 2p + 3}{p^4 + 3} = \frac{1}{p^2 + 2p + 1}$$

$$v_3(n) = 0\ 1\ 2\ 2[0] \subset \frac{p^2 + 2p + 2}{p^4} = \frac{1}{p^2 + 2p + 2}$$

$$v_4(n) = [0\ 1\ 1\ 2\ 3\ 1] \subset \frac{1}{p^2 + 3p + 3}.$$

If a_n is a zero divisor, then there is no series of which the rational function is the transform.

F. Elementary properties of the operational calculus

1) *Property of the operator: "multiplication by p"*: The operator "multiplication of p" is a *shift operator.*

$$v(n) \subset V(p) \qquad v(n+1) \subset W(p) = \sum_0^\infty \frac{v(n+1)}{p^{n+1}}$$

$$W(p) = pV(p) + v(0)$$

$$v(n+i) \subset p^i V(p) + \sum_{j=0}^{i-1} v(j)p^{i-j-1}.$$

2) *Initial and final value theorems*:

Initial value:

$$v(n)_{n=0} = [pV(p)]_{1/p=0}. \tag{8}$$

Final value: if the limit exists, i.e.,

$$V(p) = \frac{N(p)}{p^q(p-1)}$$

$$v(n)_{n\to\infty} = [(p-1)V(p)]_{p=1}. \tag{9}$$

Example (Z_3):

$$v(n) = [1\ 2] \subset \frac{p+2}{p^2+2} \qquad v(0) = \left(\frac{p^2+2p}{p^2+2}\right)_{1/p=0} = 1$$

$$v(n) = 0\ 2[1] = \frac{p^2+p+2}{p^2(p+2)} \qquad v(\infty) = \frac{1+1+2}{1} = 1.$$

3) *Translation of p*: Let us replace p with $p + \lambda$, then $V(p) \to V(p+\lambda) = W(p)$ $v(n) \to w(n)$, which can be symbolically written in the following way:

$$w(n) = v(0)\lambda^n + V(i)\cdot n\lambda^{n-1} + \cdots + V(i)C_n^i\lambda^{n-i} + \cdots + (n) \tag{10}$$

$$w(n) = [v(n) + \lambda]^n$$

where the binomial coefficients C_n^i are taken modulo k, according to the Euler triangle.

Example (Z_4):

$$v(n) = [0\ 1] \subset \frac{1}{p^2+3}$$

$$p/p-1 \qquad W(p) = V(p-1) = \frac{1}{(p-1)^2+3}$$

$$W(p) = \frac{p+2}{p^3} \supset 0\ 1\ 2[0]$$

$$w(0) = v(0) = 0$$

$$w(1) = v(1) = 1$$

$$w(2) = v(0) + 2v(1) + v(2) = 2$$

$$w(3) = v(0) + 3v(1) + 3v(2) + v(3) = 0$$

$$w(4) = v(0) + 2v(2) + v(4) = 0 \cdots .$$

4) *Derivate theorem*: Extending the usual definition of a derivate, we define:

$$\frac{dV}{dp} = -\frac{v(0)}{p^2} - \frac{2v(1)}{p^3} - \cdots (n+1)\frac{v(n)}{p^{n+2}} + \cdots$$

$$\frac{dV}{dp} \text{ modulo } k = (k-1)\frac{v(0)}{p} + (k-2)\frac{v(1)}{p^2} + \cdots (k-n-1)\frac{v(n)}{p^{n+1}}$$

$$W(p) = p\frac{dV}{dp} \supset w(n)$$

$$= [(k-1)v(0), (k-2)v(1), \cdots, (k-i-1)v_i] \cdots . \tag{11}$$

Example (Z_4):

$$v_1(n) = [0\ 1\ 2\ 3] \subset \frac{p^2+2p+3}{p^4+3}$$

$$p\frac{dV_1}{dp} = \frac{2p^2+2p}{p^4+3} \supset [0\ 2\ 2\ 0] = [3.0, 2.1, 2.2, 0.3]$$

Example (Z_2):

$$v_2(n) = [0\ 1\ 1\ 1] \subset \frac{p^2+p+1}{p^4+1}$$

$$p\frac{dV_2}{dp} = \frac{p}{p^4+1} \supset [0\ 0\ 1\ 0]$$

$$p\frac{dV}{dp} \supset (n+1)v(n) = \begin{cases} v(n) & n \text{ even} \\ 0 & n \text{ odd} \end{cases}$$

$$d\frac{(pV)}{dp} \supset nv(n) = \begin{cases} v(n) & n \text{ odd} \\ 0 & n \text{ even.} \end{cases}$$

5) *Inverse transform*:

a) the Euclidian division algorithm can be used to find the inverse transform:

$$p^q - 1 \;\frac{\dfrac{v(0)}{p} + \dfrac{v(1)}{p^2} + \cdots}{v(0)p^{q-1} + v(1)p^{q-2} + \cdots + v(q-1)}$$

$$\frac{v(0)p^{q-1} + \cdots + \dfrac{v(0)}{p}}{v(1)p^{q-2} + \cdots + v(q-1) + \dfrac{v(0)}{p}}$$

b) we can also perform derivate operations:

$$v(n) = \left\{\frac{(-1)^n}{n!}\left[\frac{d}{d^n p}\,[p^n V(p)]\right]p^{n+1}\right\}_{1/p=0}. \tag{12}$$

The operations are performed in the ring of integers Z, the results being reduced modulo k [see Section I–F–9].

Examples (Z_4):

$$V(p) = \frac{p+2}{p^2+3} \supset [1\ 2]$$

$$v(n)_{n=2} = \left\{\frac{1}{2!}\left[\frac{d}{d^2p}\left[p^2\,\frac{p+2}{p^2+3}\right]\right]\cdot p^3\right\}_{1/p=0}$$

$$\frac{d}{dp}\left(\frac{p^3+2p^2}{p^2+3}\right)$$

$$= \frac{p^4+p^2}{(p^2+3)^2}\,,\ \frac{1}{2}\frac{d}{dp}\left[\frac{p^4+p^2}{(p^2+p^3)^2}\right] = \frac{p}{(p^2+3)^2}$$

$$v(2) = \left[\frac{p}{(p^2+3)^2}\cdot p^3\right]_{1/p=0} = 1.$$

6) *Summation of* $v(n)$: Denoting $w(n) = \sum_0^n v(j)$, i.e., $w(o) = v(0)$, $w(1) = v(0) + v(1)$ we have $w(n+1) = w(n) + v(n+1)$ computing the transforms:

$$pW(p) + w(0) = W(p) + pV(p) + v(0)$$

$$W(p)(p-1) = pV(p) \tag{13}$$

$$W(p) = \frac{pV(p)}{p-1}.$$

Example (Z_3):

$$v(n) = [1\ 2] \subset \frac{p+2}{p^2+2}$$

$$W(p) = \frac{p}{p^2+2} \supset [1\ 0]$$

$$w(0) = v(0) = 1$$

$$w(1) = v(0) + v(1) = 1 + 2 = 0$$

$$w(2) = w(1) + v(2) = 1 \cdots .$$

7) *Convolution of* $v(n)$: Let us consider two sequences $v(n)$ and $w(n)$ and their transforms $V(p)$ and $W(p)$. Denote $H(p) = pV(p)W(p)$

$$H(p) = \frac{v(0)w(0)}{p} + \frac{v(0)w(1) + w(0)v(1)}{p^2} + \cdots$$

$$H(p) = \sum_{n=0}^{\infty}\sum_{i=0}^{n}\frac{v(i)w(n-i)}{p^{n+i}} \tag{14}$$

$$h(n) = \sum_{i=0}^{n} v(i)w(n-i). \tag{15}$$

Example (Z_2):

$$v_1(n) = [0\ 1] \qquad w_1(n) = [1\ 0]$$

$$H_1(p) = p\cdot\frac{1}{p^2+1}\cdot\frac{p}{p^2+1} = \frac{p^2}{p^4+1} \supset [0\ 1\ 0\ 0] = h_1(n)$$

Example (Z_4):

$$v_2(n) = [1] \qquad w_2(n) = [2] \qquad h_2(n) = [2\ 0]$$

$$H_2(p) = p\cdot\frac{1}{p+3}\cdot\frac{2}{p+3} = \frac{2p}{(p+3)^2}$$

$$= \frac{2p(p^2+2p+3)}{p^4+3} = \frac{2p}{p^2+3}.$$

8) *Convolution of* $V(p)$. *Logical product* (k prime): Our operational calculus, though applicable to linear operations, would be of little interest if it were not applicable to "nonlinear" operations. The logical product (intersection, "AND") of two binary sequences can be analyzed by these convolution properties, which, in the finite and quantized case, are more practical than in the continuous case.

Let us assume that $v(n) \subset V(p)$, $w(n) \subset W(p)$, and that $h(n) = v(n)\cdot w(n)$ (multiplication modulo k). We will write $H(p) = V(p) \otimes W(p)$ [convolution of $v(p)$ by $w(p)$].

Assume that we have expanded $V(p)$ into partial fraction $v(p) = \sum_i A_i/p + a_i$ where A_i and a_i are elements of K such that $a_i^h = 1$ [in the Galois extension of field the denominator $V(p)$], then

$$H(p) = \sum_n v(n)w(n)/p^{n+1}$$

$$H(p) = \sum_i\sum_n \frac{A_i a_i^n w(n)}{p^{n+1}}$$

$$H(p) = \sum_i \frac{A_i}{a_i}\sum_n \frac{w(n)a_i^{n+1}}{p^{n+1}} = \sum_i \frac{A_i}{a_i}\sum_n \frac{w(n)}{q^{n+1}}\ (p/a_i = q)$$

$$H(p) = \sum_i \frac{A_i}{a_i}\,w(q) \qquad q = p/a_i. \tag{16}$$

Example (Z_3):

$$v(n) = [0\ 1\ 2\ 1] \qquad w(n) = [0\ 1]$$

$$H(p) = \frac{(p^2+1)^2}{p^4+2} \otimes \frac{1}{p^2+2}\,,\quad p^2+2 = (p+1)(p+2)$$

$$\frac{1}{p^2+2} = \frac{1}{p+1} + \frac{2}{p+2}\,,$$

$$H(p = \frac{1}{2}\left[\frac{p^2+2p+1}{p^4+2}\right] + \frac{2}{1}\left[\frac{p^2+2p+1}{p^4+2}\right]$$

$$H(p) = \frac{p^2+1}{p^4+2} = \frac{1}{p^2+2} \qquad h(n) = [0\ 1].$$

Differentiation appears to be a special convolution operation:

$$\frac{-p}{1!}\frac{dV}{dp} \Rightarrow V(p) \otimes R_1(p) \qquad R_1(n) = [123 \cdots k]$$

$$\frac{p^2}{2!}\frac{d^2V}{dp^2} \Rightarrow V(p) \otimes R_2(p) \qquad R_2(n) = [136 \cdots]$$

$$\frac{(-1)p^i}{3!}\frac{d^iV}{dp^i} \Rightarrow V(p) \otimes R_i(p) \qquad R_i(n) = [1 \cdots]$$

the sequence $R_i(n)$ being the jth column of an Euler triangle.

9) *Residual classes*: The property described in this section appears to be the most important and the most interesting one. It shows that all operations can be performed in C (the field of complex numbers) provided the results are taken modulo k.

Polynomials with coefficients in Z_k are consistent with polynomials with coefficients in C modulo, a polynomial with coefficients which are multiples of k.

$$F(p) = p^h + a_{h-1}p^{h-1} + \cdots + a_{1p} + a_0$$
$$F'(p) = F(p) + h\sum_i \alpha_i p^i \qquad \alpha_i \in Z_k.$$

Thus we shall operate on the $F'(p)$ polynomials in C and subsequently take their image in Z_k (operations in C will be denoted by parentheses).

Examples:

a) (Z_2) given $V(p) = 1/p^2 + 1$, what is $v(n)$. Let us select $F(p) = F'(p) + 2p$

$$\left\{V'(p) = \frac{1}{p^2 + 2p + 1}\right\} = \left\{-\left[\frac{d}{dp}\left(\frac{1}{p+1}\right)\right]\right\}$$
$$= -\left[\frac{d}{dp}\left[\sum_{1=n}^{\infty}\frac{(-1)^n}{p^n}\right]\right] = \sum_1^{\infty}\frac{(-1)n^{n+1}}{p^{n+1}}$$

$$\{V'(p) = 1/p^2 - 2/p^3 + 3/p^4 + \cdots\}v'(n) = [(-1)^{n+1}]\cdot n.$$

Setting odd numbers to 1, even numbers to 0, and minus signs to plus signs, we get: $v(n) = [01]$.

b) Let us perform the convolution of $v(n) = [01]$ and $w(n) = [101]$ in two different ways, in Z_2 and in C.

$$C(p) = \frac{1}{p^2+1} \otimes \frac{p+1}{p^2+p+1} \qquad (a^2 + a + 1 = 0)$$

$$\frac{p+1}{p^2+p+1} = \frac{a^2}{p+a} + \frac{a}{p+a^2},$$

$$C(p) = \frac{a^2}{a\left(\frac{p^2}{a^2}+1\right)} + \frac{a}{a^2\left(\frac{p^2}{a}+1\right)}$$

$$C(p) = \frac{1}{p^4+p^2+1} = \frac{p^2+1}{p^6+1} \supset [0\,0\,0\,1\,0\,1]$$

$$\frac{1}{p^2+1} = \left\{\frac{1}{p^2+1}\right\} = \left\{\frac{1}{2}\left[\frac{i}{p+i} - \frac{i}{p-i}\right]\right\}$$

$$\left\{C(p) = \frac{1}{2}\left[\left(\frac{i}{-i}\right)\cdot\frac{-ip-1}{p^2+ip-1} - \left(\frac{i}{i}\right)\frac{ip-1}{p^2+ip-1}\right]\right\}$$

$$C(p) = \left\{\frac{-1}{p^4-p^2+1}\right\} = \frac{p^2+1}{p^6+1}.$$

This property allows us to perform all convolution operations, for all k and all periods of q.

10) *Difference equations*: Consider the following homogeneous linear difference equation

$$\sum_{i=0}^{h} a_i v(n+i) = 0$$

with initial conditions $v(j) = v_j$ $(j \leq h-1)$; we ignore the case where $v_j = 0$, $\forall_j$.

Taking the transforms:

$$\sum_0^h a_i p^i V(p) = \sum_0^h a_i \sum_0^{i-1} v_i p^{i-j-1}$$
$$V(p) = \frac{\sum_0^h a_i \sum_0^{i-1} v_i p^{i-j-1}}{\sum_0^h a_i p^i}. \tag{17}$$

Factoring out the p's:

$$V(p) = \frac{\sum_0^{h-1} p^i \sum_{m=0}^{h-i-1} a_{m+i+1}v_m}{\sum_0^K p^i a_i}.$$

let $b_i = a_{m+i+1}v_m$. The b_i' are linearly independent since $b_{h-i-1} = f(V_0V_1 \cdots V_i)$ and can be taken as new parameters

$$V(p) = \frac{\sum_0^{h-1} p^i b_i}{\sum_0^h p^i a_i} \tag{18}$$

Equation $\sum_0^h p^i a_i = 0$ is called the *characteristic equation*. According to Galois' extended theorem there exist $A(p)$ and q such that:

$$(a_k = 1,\ a_0 \neq 0) \qquad V(p) = \frac{\sum_0^{h-1} p^i b_i \cdot A(p)}{p^{q'}(p^q - 1)}$$
$$= \frac{B(p)\cdot A(p)}{p^{q'}(p^q-1)} \quad (q, q' \leq k^h - 1).$$

Theorem 1: The sequence solutions of a linear difference equation of degree h is ultimately periodic of maximum period $k^h - 1$.

Theorem 2: All the sequences' solutions for different initial values can be obtained from the polynomial $A(p)$, complementary of the characteristic polynomial, by linear combination of the h polynomials, $p^i A(p)$, $[0 < i < h - 1]$.

Example (Z_2):

$$v(n+3) + v(n+1) + v(n) = 0 \quad (v_0, v_1, v_2, \text{ given}).$$

Taking the transforms

$$p^3V(p) + v_0p^2 + v_1p + v_2 + pV(p) + v_0 + V(p) = 0$$

$$V(p) = \frac{p^2v_0 + p(v_0 + v_1) + v_2}{p^3 + p + 1}$$

$$V(p) = \frac{(p^2b_2 + p^1b_1 + b_0)(p^4 + p^2 + p + 1)}{p^7 + 1}$$

$$= \frac{B(p)\cdot A(p)}{p^7 + 1} = \frac{C(p)}{p^7 + 1}.$$

Nonhomogeneous equations can be written under the following form:

$$\sum_{i=0}^{h} a_i v(n+i) = \sum_{j=0}^{h'} b_j w(n+j) \tag{19}$$

where $w(n)$ is a known forcing function.

$$V(p) = \frac{V[p, v(0), v(1), \cdots v(h-1), w(0), w(1), \cdots w(h'-1)]}{\sum_{0}^{h} a_i p^i} \tag{20}$$

Example (Z_4):

a)

$$v(n+2) + 2v(n+1) + 3v(n) = w(n+1) + w(n)$$

$$v(0) = v(1) = 0, \qquad w(n) = [0\ 1\ 2\ 3] \subset \frac{1}{p^2 + 2p + 1}$$

$$V(p) = (p^2 + 2p + 3) = W(p)(p+1) = \frac{p+1}{p^2 + 2p + 1}$$

$$V(p) = \frac{p+1}{p^4 + 3} \supset [0\ 0\ 1\ 1].$$

b)

$$v(n+2) + 2v(n+1) + 2v(n) = 1, \qquad v(0) = v(1) = 0$$

$$V(p)(p^2 + 2p + 2) = \frac{1}{p+3}$$

$$V(p) = \frac{1}{(p+3)(p^2 + 2p + 2)}$$

$$= \frac{p^2 + 2p + 2}{p^4(p+3)} = \frac{1}{p+3} + \frac{3p^3 + 3p^2 + 2}{p^4}$$

$$v(n) = \underbrace{0\ 0\ 1\ 3}_{\text{Transient}}\ \underbrace{[1]}_{\text{Steady-state solution.}}$$

G. Connections with Z transform

Our operational calculus is analogous to the discrete transformation Laplace called the "generating function" from which all modern discrete transforms issue [5]. Using the same definition of the transform $V(p)$, and operating in the complex field C we obtain

$$v(n) \epsilon C = [v(0) \cdots v(q-1)], \tag{21}$$

$$V(p) = \frac{v(0)p^{q-1} + v(1)p^{q-2} + \cdots + v(q-1)}{p^q - 1}$$

if we exclude the fact that the summation operation is to be taken modulo k, the canonical expression (4) is formally identical to (21). If the quantization step goes to zero, $k \to \infty$, the expresssion $V_k(p)$ $(k \to \infty)$ is equivalent to the Z transform of $V(n)$.

$$V_k(p) = \sum_{0}^{\infty} \frac{v(n)}{p^{n+1}} \Rightarrow \mathbf{V}(Z) = \sum_{0}^{\infty} v(nT)Z^{-n}$$

$$\mathbf{V}(Z) = [pV_k(p)]_{p=z} \qquad k \to \infty.$$

Let us consider, for instance, the q-periodic sequence $(\epsilon Z_k)v$ such that :

$$v(n) = [v(0), \cdots v(q-1)] \qquad V(p) = \frac{V(p)}{p^q - 1}.$$

We can expand $V(n)$ into *discrete Fourier series* or expand $V(p)$ (ϵC) into partial fractions:

$$V(p) = \frac{V(p)}{p^q - 1} = \sum_{h=0}^{n-1} \frac{A_h(p)}{p - e^{\frac{2h\pi_j}{q}}} \tag{22}$$

$$V(p) = \sum_{0}^{n-1} \frac{B_h(p)}{p^2 + 2p\cos\frac{2h\pi}{q} + 1}.$$

Equation (22) is analogous to the Z transform of $v(n)$.[3]

$$\mathbf{V}(Z) = \frac{Z(aZ + b)}{Z^2 - 2Z\cos wT + 1}$$

$$\rightarrow V(p) = \frac{ap + b}{p^2 - 2p\cos\frac{2h\pi}{q} + 1}$$

where

$$wT = \frac{2h\pi}{q}\ (Z)^4.$$

Example:

$$v(n) = [0\ 1\ 2] \qquad v(n)\ \epsilon\ Z_k \qquad K > 2$$

$$V_k(p) = \frac{p+2}{p^3 - 1} \text{ (summation modulo } k).$$

[3] Is Galois' theorem valid for $k \infty$? If the roots of $G(p)(\epsilon C)$ are also roots of $p^q - 1$, there exist $C(p)$ such that $G(p)C(p) = p^q - 1$.

[4] If the period of $V(t)$ is a multiple of the sampling period, then $v(nT)$ is periodic, $V(p)$ is a rational function, and the poles of $\mathbf{V}(z)$ have rational abscissas on the unit circle.

If

$$k \to \infty \qquad V_k \to V_\infty \qquad V_\infty = \frac{p+2}{p^3+1}$$

(ordinary summation)

$$V_\infty(p) = \frac{1}{p-1} + \frac{1}{3}\left[\frac{1-e^{2\pi i/3}}{p-e^{2\pi i/3}} + \frac{1-e^{-2\pi i/3}}{p-e^{-2\pi i/3}}\right]$$

$$= \frac{1}{p-1} - \frac{p+1}{p^2 - 2p\cos\frac{2\pi}{3} + 1}$$

$$\mathbf{V}(Z) = [pV_\infty(p)]_{p=Z} = \frac{Z}{Z-1} - \frac{Z^2+Z}{Z^2 - 2Z\cos\frac{2\pi}{3} + 1}$$

$$\mathbf{V}(Z) = \frac{Z}{Z-1} - \frac{Z^2 - Z\sin 2\pi/3}{Z^2 - 2Z\cos 2\pi/3 + 1} - \frac{\sqrt{3}}{3}\frac{Z/2}{Z^2 - 2Z\cos 2\pi/3 + 1}$$

$$v(n) = 1 - \cos(2\pi/3)n - \frac{\sqrt{3}}{3}\sin(2\pi/3)n = [0\ 1\ 2].$$

II. Linear Sequential System

A. The transfer function of a linear sequential system

Let us consider a linear sequential system which is input invariant. Suppose that for an input $e(n)$ it is possible to consider an output $s(n)$

$$e(n) \to S(n) \qquad e(n+i) \to S(n+i) \qquad \forall i > 0$$

$$\lambda e(n) \to \lambda S(n)$$

$$e(n) = e_1(n) + e_2(n) \to S(n) = S_1(n) + S_2(n).$$

Assuming $e(n) = \delta(n-i)$, $e(n) = 1$, $n = i$, $e(n) = 0$ $n \neq i$, and that $h(n)$ is the output corresponding to $\delta(n)$, $\delta(n-i) \to h(n-i)$ the response to $e(i)$ $\delta(n-i) = e(n)$ is $e(i)h(n-i)$, the response to the general input

$$e(n) = \sum_0^\infty \delta(n-i)e(i)$$

is

$$S(n) = \sum_{i=0}^{i=n} e(i)h(n-i).$$

Using the convolution theorem [Section I–F–7] we have

$$S(p) = pE(p)H(p).$$

If we call $p \cdot H(p) = G(p)$ the *transfer function* of the system, we have

$$S(p) = G(p) \cdot E(p). \tag{23}$$

Note: $e(n) = \delta(n) \subset 1/p$, $S(p) = p \cdot 1/p = H(p)$ which is consistent with the definition of $h(n)$.

B. Elementary operators

Adder: the adder is a combinational device with one output $s(n)$ and different inputs $e_i(n)$ such that:

$$S(n) = \sum e_i(n) \qquad \text{(modulo } k \text{ sum)}.$$

Multiplier: the multiplier is a combinational device with one output $s(n)$ and one input $e(n)$ such that:

$$S(n) = \lambda e(n) \quad \lambda \in Z_k \text{ (modulo } k \text{ product)}.$$

Shift register: the shift register is a sequential device with one input $e(n)$ and one output $s(n)$ such that:

$$S(p) = E(p)/p.$$

C. Passive systems

A linear system is called passive if its transfer function is a rational function:

$$G(p) = \frac{N(p)}{D(p)}$$

where degree of $N(p) \leq$ degree of $D(p)$.

Theorem: *Passive systems are physically realizable with modulo k adders, multipliers, and shift registers.*

Proof: Assume that

$$G(p) = \frac{a_n p^n + a_{n-1}p^{n-1} + \cdots + a_0}{p^n + b_{n-1}p^{n-1} + \cdots + b_0}.$$

$G(p)$ is the transfer function of the system of Fig. 1.

$$G(p) = \frac{a_n + a_{n-1}/p + \cdots + a_0/p^n}{1 + b_{n-1}/p + \cdots + b_0/p^n} = \frac{S(p)}{E(p)}$$

$$S(p) = \epsilon(p)\left(a_n + \frac{a_{n-1}}{p} + \cdots + \frac{a_0}{p^n}\right)$$

$$\epsilon(p) = E(p) - \epsilon(p)\left(\frac{b_{n-1}}{p} + \cdots + \frac{b_0}{p}\right)$$

$$E(p) = \epsilon(p)\left(1 + \frac{b_{n-1}}{p} + \cdots + \frac{b_0}{p}\right).$$

Hence

$$S(p) = \frac{a_n + a_{n-1}/p + \cdots + a_0/p}{1 + b_{n-1}/p + \cdots + b_0/p}.$$

Example (Z_4) [see Section I–F–10 and Fig. 2]:

$$G(p) = \frac{p^2+2p+2}{p^4} = \frac{1}{p^2+2p+2}$$

$$E(p) = \frac{1}{p+3} \supset [1]$$

$$S(p) = \frac{p^2+2p+3}{p^2(p+3)}.$$

Note a): Consider the block diagram of Fig. 3 and assume that $G(p) = 1$, $H(p) = 1/p + 1$ (over Z_2). We have $S/E = G(p)/[1 + H(p)G(p)] = p$, $S(n) = e(n+1)$. Hence we have synthetized a *predictor*. This is an evident absurdity. Assume that all values of the variables of the system are zero, and consider the sequence $e(n) = \delta(n) = 1[0]$

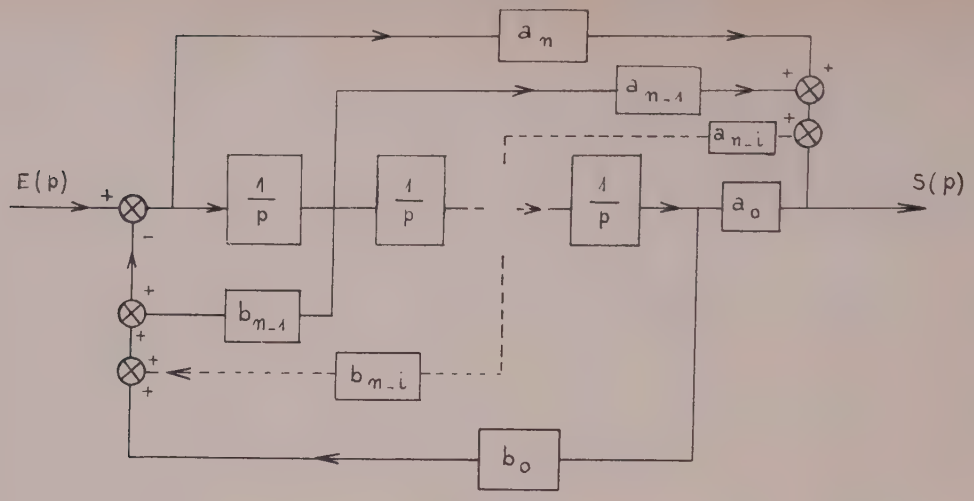

Fig. 1.

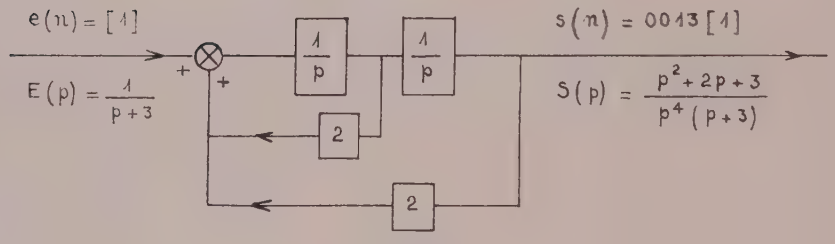

Fig. 2.

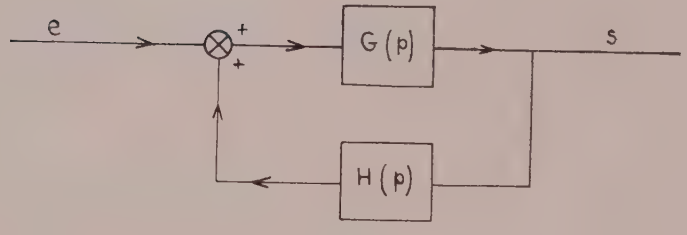

Fig. 3.

$$S(0) = e(0) + S(0) + S(-1)$$

$$S(0) = e(0) + S(0) = 1 + S(0).$$

This equation is meaningless, since the output is neither 0 nor 1. The system is physically unrealizable. *A block diagram with a feedback loop which does not contain a shift register is physically unrealizable.*

Note b): the classical state variable representation [12] is also applicable to linear modulo k sequential systems. It easily can be shown that it is possible to go from the transfer function to the state variable representation and conversely.

D. Eigenfunction problem

We will say that $E(p)/p^q - 1$ is a *strict eigenfunction* for the linear sequential system (modulo k) of transfer function $N(p)/D(p)$ if the output $S(p)$ is such that

$$S(p) = \frac{E(p)}{p^q - 1} + \frac{B(p)}{p^n}. \tag{24}$$

If $E(p)$ exists, we then have

$$\frac{E(p)}{p^q - 1} + \frac{B(p)}{p^n} = \frac{E(p)}{p^q - 1} \cdot \frac{N(p)}{D(p)}$$

$$\frac{E(p)}{p^q - 1} = \frac{B(p)D(p)}{p^n[N(p) - D(p)]}.$$

Since $B(p)$ is not divisible by p^n, $D(p)$ should be $D(p) = p^n D'(p)$. There exists at least one polynomial $C(p)$ such that

$$[N(p) - D(p)]C(p) = p^q - 1.$$

Then, given a transfer function $N(p)/p^n D'(p)$ with

$$[N(p) + p^n D'(p)] \cdot C(p) = p^q - 1 \qquad (N(0) \neq 0)$$

the eigenfunction in the strict sense of the corresponding system is

$$\frac{E(p)}{p^q - 1} = \frac{B(p)D'(p)C(p)}{p^q - 1}. \tag{25}$$

Example (Z_2):

$$\frac{N(p)}{D(p)} = \frac{1}{p(p^2+p+1)}, \quad B(p) = 1, \quad n = 1$$

$$\frac{E(p)}{p^4-1} = \frac{p(p^2+p+1)}{p(1+p^3+p^2+p)} = \frac{p^3+1}{p^4+1}.$$

Verification:

$$\frac{p^3+1}{p^4+1}\cdot\frac{1}{p(p^2+p+1)} = \frac{p+1}{(p^4+1)p} = \frac{1}{p} + \frac{p^3+1}{p^4+1}.$$

Similarly we will say that $E(p)/p^q - 1$ is an *eigenfunction in a broad sense* if the output $S(p)$ is:

$$S(p) = \frac{E(p)}{p^r(p^q-1)} + \frac{B(p)}{p^n} \qquad r < q,$$

If $E(p)$ exists

$$\frac{E(p)}{(p^r-1)p^q} + \frac{B(p)}{p^n} = \frac{N(p)}{D(p)}\cdot\frac{E(p)}{(p^q-1)}$$

$$\frac{E(p)}{p^q-1} = \frac{B(p)D(p)p^r}{p^n(N(p)p^q - D(p)}. \tag{25}$$

If $D(0) \neq 0$, for any $r > 0$ there is always at least one set of eigenfunctions ($r = n$)

$$\frac{E(p)}{p^q-1} = \frac{B(p)\ D(p)}{N(p)p^q - D(p)}.$$

If

$$D(p) = p^s D'(p) \quad \frac{E(p)}{p^q-1} = \frac{B(p)D'(p)p^{r+s}}{p^n[N(p)p^q - D(p)]}$$

n can always be choosen in such a way that $n = r + s$.

$$\frac{E(p)}{p^q-1} = \frac{B(p)D'(p)C(p)}{p^q-1}. \tag{26}$$

Example (Z_2):

$$\frac{N(p)}{D(p)} = \frac{p}{p^2+1} \quad n = r = 2 \qquad B(p) \equiv 1$$

$$\frac{E(p)}{p^q-1} = \frac{(p^2+1)p^2}{p^2(p^3+p^2+1)} = \frac{p^6+p^5+p^2+1}{p^7+1}.$$

Verification (see Fig. 4):

$$\frac{p^2+1}{p^3+p^2+1}\cdot\frac{p}{p^2+1} = \frac{p^5+p^4+p^3+p}{p^7+1}.$$

The pattern of 0's and 1's of the input is *cyclicly unchanged*, but is shifted r-places to the right. In the previous example [1101001] becomes [0111010] after two cyclic shifts.

E. Applications

1) *Sequence generator*: Given an oscillator whose output is a reference periodic sequence $s(n) = [1]$, it is possible to obtain from it, through the convenient passive filter $H(p)$, any desired ultimately periodic sequence $\subset U(p)\cdot$ ($u(n) \in Z_K$) (see Fig. 5).

$H(p)$ is the transfer function of a realizable passive system, since

$$H(p) = \frac{[p^{r+q-1}a(0) + \cdots a(r+q-1)](p-1)}{p^r(p^q-1)} = \frac{N'(p)}{D(p)}$$

degree of $N'(p) \leq$ degree of $D(p)$.

2) *Linear coding* (Z_K): All linear codes (Boolean or *not Boolean*) can be expressed by means of this operational calculus and transfer function representation, which turn out to be much more practical than the classical matricial apparatus. Analysis and synthesis are equally feasible. The problem of linear coding is then reduced to the well-known problem of linear filtering.

Let us consider the linear system of Fig. 6.

$$S(p) = \frac{C(p)}{p^n}\cdot\frac{m(p)}{p^n} \qquad R(p) = S(p) + E(p)$$

$$M(p) = R(p)\cdot\frac{1}{C(p)} = \left[\frac{C(p)}{p^{n+n}}\,m(p) + E(p)\right]\frac{1}{C(p)}.$$

The output $S(p)$ of the first box is divided by $C(p)$ which selects thereby the coded message in a certain subspace space. If the transmitted message is not in this subspace, then an error occured in transmission.

If there is no error $E(p) = 0$, $M(p) = m(p)/p^{n+n}$. Then the message appears as: $\underbrace{00\cdots0}_{h}\, m_1 m_2 \cdots m_n 000 \cdots$

It is characterized by the presence of 0's after the $(n+n)$th digit.

If $E(p) = C(p)m'(p)/p^{n+n}$, the error is in the subspace and cannot be detected. The linear coding problem is closely related with the eigenfunction problem. However, this paper will not present a discussion of the matter; it will simply show how the tool introduced can help to improve understanding, and how easily it permits realization of the coding and decoding devices.

If the polynomial $C(p)$ is a primitive polynomial [18], then for a given number of shift registers the transmitted message is the longest. We will call such a code (with analogy to the Boolean case), a simple Hamming code. Let us take, for example:

$$C(p) = p^2 + p + 2 \quad (Z_3)$$

$$D(p) = (p^6 + 2p^5 + 2p^4 + 2p^2 + p + 1)$$

$$C(p).\ D(p) = p^{3^2-1} - 1 = p^8 - 1$$

$$m(p) = m(0)p^5 + \cdots + m_5$$

$$E(p) = \frac{e(0)p^6 + \cdots + e(6)}{p^8}$$

$$S(p) = \frac{m(p)}{p^6}\cdot\frac{p^2+p+2}{p^2}$$

$$M(p) = \frac{m(p)}{p^8} + \frac{E(p)}{p^8(p^2+p+2)}$$

$$M(p) = \frac{m(p)}{p^8} + \frac{E(p)\ D(p)}{p^8(p^8+2)} = \frac{m(p)}{p^8} + \frac{A(p)}{p^8} + \frac{B(p)}{p^8+2}$$

with degree of $A(p)$ and $B(p) \leq 7$.

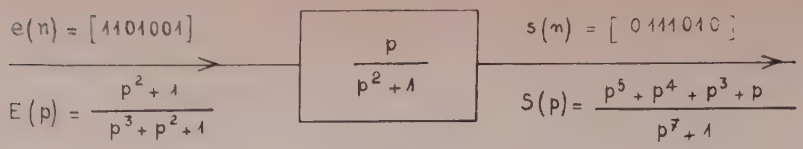

Fig. 4.

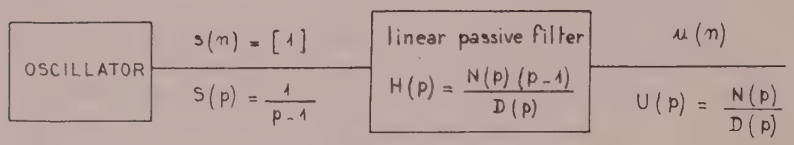

Fig. 5.

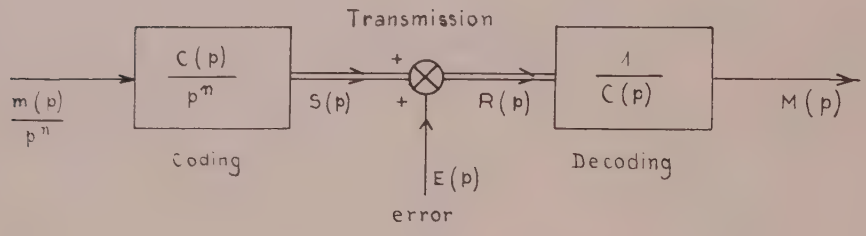

Fig. 6.

3) *Error detection and correction*: we assume that the error is of the following type:

$$E(p) = \frac{p^i}{p^8} \qquad 0 \le i \le 7$$

$$\frac{p^i D(p)}{p^8(p^2 + p + 2)} = \frac{A(p)}{p^8} + \frac{B(p)}{p^8 + 2}.$$

The equation can be rewritten as the *decoding equation*

$$A(p)(p^8 - 1) + B(p)p^8 = p^i \cdot D(p).$$

Let a be a root of $D(p)(D(a) = 0)$, a is also a root of the polynomial $p^8 - 1$, thus $B(a) = 0$: all the roots of $D(p)$ are roots of $B(p)$. Since $D(p)$ is of degree 6 and $B(p)$ of degree 7, $B(p)$ is such that

$$B(p) = D(p)(\alpha_1 p + \alpha_0).$$

The decoding equation (27) becomes

$$A(p)(p^2 + p + 2) + p^8(\alpha_1 p + \alpha_0) = p^i. \qquad (28)$$

Let a be a root of the coding polynomial $p^2 + p + 2$. $(a^8 = 1)$, $a^2 + a + 2 = 0$, a is a primitive element, and a^3 is the other root. Thus:

$$p^2 + p + 2 = (p - a)(p - a^3) = p^2 - p(a + a^3) + a^4.$$

Then let $p = a, a^3$ in (28)

$$\begin{aligned} a^i &= a^8(\alpha_1 a + \alpha_0) = \alpha_1 a + \alpha_0 \\ a^{3i} &= a^{24}(\alpha_1 a^3 + \alpha_0) = \alpha_1 a^3 + \alpha_0. \end{aligned} \qquad (29)$$

The α's are determined in a unique way from the position of the error and conversely. $B(p)$ is completely determined by the periodic pattern of the output, as are the α's from which we obtain the position i of the error.

Solving (29) we obtain

$$\alpha_1 = \frac{a^i - a^{3i}}{a^2} \qquad \alpha_0 = \frac{a^{i+1} + a^{3i} - a^i}{a}.$$

From Table I, it appears that the pattern of the periodic sequence of the output is cyclicly shifted to the left of i places from the original pattern of the polynomial $D(p)$.

TABLE I

error position	α_0	α_1	Pattern of the periodic sequence: $B(p)$						
0	0	1	0	1	2	2	0	2	1	1
1	1	0	1	2	2	0	2	1	1	0
2	2	1	2	2	0	2	1	1	0	1
3	2	2	2	0	2	1	1	0	1	2
4	0	2	0	2	1	1	0	1	2	2
5	2	0	2	1	1	0	1	2	2	0
6	1	2	1	1	0	1	2	2	0	2

Example (Fig. 7):

$$m(p) = p^5 + 2p^4 + 1$$

$$S(p) = \frac{m(p)(p^2 + p + 2)}{p^8} = \frac{p^7 + p^5 + p^4 + p^2 + p + 2}{p^8}$$

$$E(p) = \frac{1}{p^4}$$

$$M(p) = \frac{p^7 + p^5 + 2p^4 + p^2 + p + 2}{p^8(p^2 + p + 2)}$$

$$M(p) = \frac{H(p)}{p^8} + \frac{C}{p - a} + \frac{d}{p - a^3}$$

$$= \frac{p^7 + p^5 + 2p^4 + p^2 + p + 2}{p^8(p^2 + p + 2)}.$$

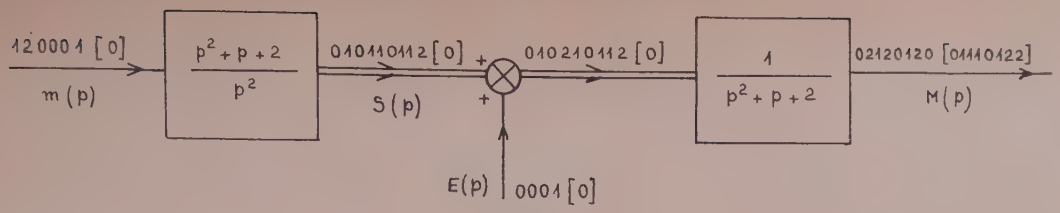

Fig. 7.

Multiplying by $(p - a)$, $(p - a^3)$ and setting $p = a$, a^3 we obtain

$$c = a^2 \qquad d = a^6$$

$$M(p) = \frac{M(p)}{p^8} + \frac{2}{p^2 + p + 1}$$

from Table I

$$\alpha_1 = 0 \qquad \alpha_0 = 2 \rightarrow i = 4.$$

Conclusion

Using the Galois extension of fields and the formal series theory, it is possible to introduce a rigorous operational calculus. It is applicable to finite or ultimately periodic sequences of elements from a finite field or ring (Z_k, K prime or not). This operational calculus is analogous and consistent with Laplace and z transformations. This tool, combined with the transfer function representation, is shown to be practical for binary sequence manipulation, and the analysis and synthesis of quantized systems.

Acknowledgment

The author is very grateful to Prof. J. C. Gille who made this research possible within the activities of the Centre d'Etudes et de Recherches en Automatisme, Ecole Nationale Supérieure de l'Aéronautique, Paris; Prof. J. A. Ville from the Econometry Department of the University of Paris, for his helpful suggestions concerning different topics in this paper; Prof. M. Houdebine from the Mathematics Department of the University of Rennes, for his valuable aid in the higher algebraic manipulations; Prof. A Gill, from the University of California, Berkeley, who kindly reviewed this paper. He also expresses gratitude to Prof. L. A. Zadeh of the University of California, Berkeley, who fostered this study through his teaching.

References

[1] E. Galois, *Ecrit et Memoirs Mathematiques*, R. Bourque and J. P. Azra, Eds. Paris: Gauthier–Villars, 1962.
[2] N. Bourbaki, *Elements de Mathematiques*, vol. III (Algebra). Paris: Hermmann, 1959.
[3] R. Carmichael, *Introduction to the Theory of Groups of Finite Order*. New York: Dover, 1956.
[4] A. A. Albert, *Fundamental Concepts of Higher Algebra*. Chicago: The University of Chicago Press, 1956.
[5] P. Montel, *Leçons sur les Récurrences et leurs Applications*. Paris: Gauthier–Villars, 1957.
[6] D. A. Huffman, "The synthesis of linear sequential coding networks," *Proc. 3rd London Symp. on Information Theory*, pp. 77–95, September 1955.
[7] ——, "A linear circuit view-point on error correcting codes," *IRE Trans. on Information Theory*, vol. IT-2, pp. 20–28, March 1956.
[8] S. W. Golomb, "Sequences with randomness properties," G. L. Martin Co., Baltimore, Md., Final Rept. on Contract 54–36611, 1955.
[9] B. Elspas, "The theory of automonous linear sequential networks," *IRE Trans. on Circuit Theory*, vol. CT–6, pp. 45–60, March 1959.
[10] T. L. Booth, "An analytical representation of signals in sequential networks," *Proc. Symp. on Mathematical Theory of Automata*. Brooklyn, N. Y.: Polytechnic Press, Polytechnic Institute of Brooklyn, April 1962.
[11] L. A. Zadeh, "From circuit theory to system theory," *Proc. IRE*, vol. 50, pp. 856–865, May 1962.
[12] ——, "An introduction to state-space techniques," 1962 Joint Automatic Control Conference.
[13] J. H. Green, Jr., and R. L. San Soucie, "An error-correcting encoder and decoder of high efficiency," *Proc. IRE*, vol. 46, pp. 1741–1744, October 1958.
[14] B. Friedland and T. E. Stern, "On periodicity of states in linear modular sequential circuits," *IRE Trans. on Information Theory (Correspondence)*, vol. IT–5, pp. 136–137, September 1959.
[15] J. E. Meggitt, "Error correcting codes for correcting bursts of errors," *IBM J. Res. and Dev.*, vol. 4, pp. 329–334, 1960.
[16] N. Zierler, "On decoding linear error correcting codes," presented at the 4th London Symp. on Information Theory, August 1960.
[17] B. Friedland, "Linear modular sequential circuits," *IRE Trans. on Circuit Theory*, vol. CT–6, pp. 61–68, March 1959.
[18] N. M. Abramson, "Error correcting codes from linear sequential circuit," in *Information Theory*, C. Cherry, Ed. London: Butterworth, 1961, pp. 26–40.
[19] W. W. Peterson, *Error Correcting Codes*. New York: Wiley, 1961.
[20] J. M. Wozencraft and B. Reiffen, *Sequential Decoding*. New York: Wiley, 1961.
[21] J. Richalet, "Calcul Operationnel Booleen," in *L'Onde Electrique*, no. 439, pp. 1003–1012, October 1963.
[22] J. Richalet, "Les Systemes Discrets," in *L'Onde Electrique*, no. 451, pp. 1011–1020, October 1964.